Proceedings of Cloud based International Conference
"Computational Systems for Health and Sustainability"
15th January, 2021 Organized by sbytetechnologies.com

Literature Study On Cloud Based Healthcare File Protection Algorithms

SAHANA SRIDHAR
Asst. System Engineer Trainee, TCS, Chennai
Email : sahayesyes@gmail.com

Abstract: **There is a huge development in Computers and Cloud computing technology, the trend in recent years is to outsource information storage on Cloud-based services. The cloud provides large storage space. Cloud-based service providers such as Dropbox, Google Drive, are providing users with infinite and low-cost storage. In this project we aim at presenting a protection method through by encrypting and decrypting the files to provide enhanced level of protection. To encrypt the file that we upload in cloud, we make use of double encryption technique. The file is been encrypted twice one followed by the other using two algorithms. The order in which the algorithms are used is that, the file is first encrypted using AES algorithm, now this file will be in the encrypted format and this encrypted file is again encrypted using RSA algorithm. The corresponding keys are been generated during the execution of the algorithm. This is done in order to increase the security level. The various parameters that we have considered here are security level, speed, data confidentiality, data integrity and cipher text size. Our project is more efficient as it satisfies all the parameters whereas the conventional methods failed to do so. The Cloud we used is Dropbox to store the content of the file which is in the encrypted format using AES and RSA algorithms and corresponding key is generated which can be used to decrypt the file. While uploading the file the double encryption technique is been implemented.**

INTRODUCTION

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing means that instead of having all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it is provided to you as a service by another company and accessed over the Internet, usually in a completely seamless way. Using cloud you will not know where the hardware and software is exactly located and how it all works does not matter. According to the user it is just somewhere up in the nebulous "cloud". As there is a huge development of computers and Cloud computing technology, the recent trend is to outsource information storage. The Cloud-based services for individual end users mainly focuses on data storage. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. The services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Software as a service (SaaS): is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software". SaaS is typically accessed by users using a thin client. Platform as a Service (PaaS): platform-based service is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. Infrastructure as a service (IaaS): are online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. A hypervisor, such as Xen, Oracle runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. Linux containers run in isolated partitions of a single Linux kernel running directly on the physical hardware. IaaS-cloud providers supply these resources on-demand from their large pools of equipment installed in data centres. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks). To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, database, and web server. In the software as a service (SaaS) model, users gain access to application software and databases. Cloud

ISSN 2320 –5547
International Journal of Innovative Technology and Research

providers manage the infrastructure and platforms that run the applications. In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud computing is beneficial to many enterprises. It lowers costs and allows them to focus on competence instead of on matters of IT and infrastructure and disadvantages, especially for smaller business operations, particularly regarding security and downtime. Thereby cloud computing has a lot of applications right from the individual users till business people.

LITERATURE SURVEY

Data over collection problem

Yibin Li et. al, (2016) focussed on the data over collection problem. They proposed to put all users' data into a cloud, the security of users' data could be greatly improved. They have done extensive experiments and the experimental results have demonstrated the effectiveness of their approach. Their most direct improvement was saving storage space in users' smartphones. The native data includes photos, music, movies, videos and other data except app data and system used data. It is obvious that those occupies more storage spaces and that could be vacated to allow users to install more apps. They presented an active approach where every app that wanted to use users' data sent its request for accessing to the cloud, and the cloud access control service could provide detailed permissions for every app to every block of users' data. Meanwhile the operations of encryption and decryption were achieved by cloud encryption/decryption service that saves computation resource of smartphone for dealing with these complex calculations. Finally, experimental result verifies the feasibility and advantages of our framework. Liwei Kuang et. al (2015), presented an efficient approach that could securely process large scale heterogeneous data securely decompose a tensor. Tensor is a mathematical model widely used in data-intensive applications. The core tensor is multiplied with a certain number of truncated orthogonal bases. The unstructured, semi-structured, and structured data are represented as low-order sub-tensors which are then encrypted using the fully homomorphic encryption scheme. A unified high-order cipher tensor model is constructed by collecting all the cipher sub-tensors and embedding them to a base tensor space. The cipher tensor is decomposed through a proposed secure algorithm, in which the square root operations are eliminated during the Lanczos procedure. The various characteristics that are been measured are n terms of time complexity, memory usage, decomposition accuracy, and data security. The result demonstrated that the approach can securely decompose a tensor with fully homomorphic encryption scheme and it is feasible. It could secure data processing on cloud.

Security authentication scheme

Jun Wu et. al (2018), proposed security authentication scheme for cluster management. Cluster management technology monitors all types of events and must maintain a consistent global network status, which usually leads to big data in SDNs. The proposed scheme is significant in improving the security and efficiency SDN control plane. In large-scale SDN, multiple controllers in the control plane must be able to collaborate to manage the entire network. Control plane extensibility is an important issue. Clustering is a feasible and proven approach to achieve efficient SDN management, in which the cluster monitors all types of events and maintain a consistent global network status. This usually involves big data in SDN. A secure authentication scheme was proposed to ensure the legality of the data sources. This work is significant in improving the performance and efficiency of applications running in SDN. In future work, a distributed security data storage scheme for the SDN controller cluster will be proposed. Krikor et. al (2009), presented a method for image encryption by selecting higher frequencies of DCT coefficient which are characteristic values for encryption. The proposed encryption method by them is selective encryption algorithm where the DC coefficients and some selective AC coefficients are encrypted. Here DC coefficients carry important visual information. The algorithm will not encrypt image bit by bit but only selective DCT coefficients are encrypted. The extra security is added to the resultant encrypted block through block shuffling method. The DCT transform is used because it minimizes the amount of data needed to recreate the digitized image.

image content recovery method

Han qui et. al (2019), proposed an image content recovery method for jpeg images that can recover the image content by estimating the DC coefficient without any pre-known knowledge. They consider certain issues such as security fault tolerance and error resistance. They used smart image processing techniques to recover the image from the loss on the receiver's end which improves the error resistance capacity for the WSN. Most of the today's multimedia data are compressed using DCT. This paper presented the DC recovery

method for jpeg images which resisted the transmission error at the execution end. Andreas Pommer et. al (2003), proposed a WP-based selective encryption scheme to provide confidentiality for retrieval-based visual communications. The usage of classical ciphers on the multimedia is proved to be inefficient as it requires high computation . They are designed to protect multimedia content and fulfil the security requirements for a particular multimedia application. Rate-distortion performance is guaranteed by a restriction of admissible WP trees, and the security analysis shows that it is very likely that the security of the cipher in use is the lower bound for attack complexity of the overall system. Med Karim Abdmouleh et. al (2017), presented that Data confidentiality and Authenticity are very much important. In that paper he proposed to use the approach of partial encryption on DWT which is compatible for JPEG2000. Using DWT, image can be decomposed into any level of subband images. This methodology is combined with Selective Encryption where after decomposition most of the information is present in the LL band. This LL band are been encrypted using the conventional encryption methods as mentioned . The advantage of this approach is that it is more faster, robust, efficient.

Cognitive radio network (**CRN**)

Keke Gai et. al, (2017) presented the cognitive radio network (CRN) which is one of the widely deployed wireless networking approaches. The communication security is a major concern while CRN is used in WSGNs. Currently, jamming and spoofing are two common attack approaches that are active in the deployment of WSGNs when using CRNs. They proposed an attack strategy, maximum attacking strategy using spoofing and jamming (MASS-SJ), which utilized an optimal power distribution to maximize the adversarial effects. Spoofing and jamming attacks are launched in a dynamic manner in order to interfere with the maximum number of signal channels. Their proposed approach had been evaluated by their experiments and the results have shown the positive performance of using MAS-SJ. H. Qiu et. al (2015), presented that Storage optimization is considered as special case of secure storage from end users to clouds. For most SE methods, the fragmentation concept is not designed based on the storage usage of public clouds which optimizes the storage usage of public clouds which optimize the storage space usage of trusted area . In brief review, only the work shown could be used to optimize the trusted storage area by uploading the public fragments to the clouds. In this paper, we define the confidential levels of the fragments and the public fragments are also protected. Thus the small private fragment with high confidential level can be stored in an area trusted by the end users while the public on and protected fragments can be stored in public clouds with resistance to attacks. Zafar Shahid et. al (2014), presented a scheme for format compliant visual protection of HEVC using selective encryption. It started with an in-depth analysis of HEVC-CABAC from an encryption standpoint. It is followed by the proposed algorithm for SE of HEVC, which satisfied all the real-time constraints, including conversion of non-dyadic ES to dyadic ES. The SE is performed on the entropy slices independently in HEVC. In this way, the proposed SE method does not affect the parallelism of HEVC. The experiments have shown that they achieved the desired level of protection both for texture information using SE of QTC syntax elements and motion information using SE of MVD syntax elements with a minimal set of computational requirements.

Secure MQ coder (SMQ) for efficient selective encryption of JPEG 2000 images.

Tao Xiang et. al (2014), presented a secure MQ coder (SMQ) for efficient selective encryption of JPEG 2000 images. SMQ only selectively encrypts tiny and constant volume of data in JPEG 2000 coding regardless of image size. Theoretical analysis and experimental results show that SMQ can achieve a balance between security and efficiency. In SMQ, encryption process is seamlessly embedded into JPEG 2000 coding process by securely disturbing the probability estimation table of MQ coder. A nonce is introduced into the generation of keystream and makes the proposed SMQ immune from chosen plaintext attacks. It is found that SMQ can get an optimal balance between security and efficiency; at the same time, it has negligible impact on compression performance and energy consumption of standard JPEG 2000 coding. Yibin L et. al (2017), proposed an intelligent cryptography approach, by which the cloud service operators cannot directly reach partial data. An alternative approach is designed to determine whether the data packets need a split in order to shorten the operation time. Their experimental evaluations have assessed both security and efficiency performances and the experimental results depict that our approach can effectively defend main threats from clouds and requires with an acceptable computation time. This paper focused on the problem of the cloud data storage and aimed to provide an approach that could avoid the cloud operators reaching user' sensitive data. In this model, they used proposed algorithms, including Alternative Data Distribution (AD2), Secure

Efficient Data Distributions (SED2) and Efficient Data Conflation (EDCon) algorithms. The computation time was shorter than current active approaches. Future work would address securing data duplications in order to increase the level of data availability since any of datacenter's down will cause the failure of data retrievals.

DCT based SE methods,

Han Qiu et. al (2018), presented the DCT based SE methods, is used for image protection especially bitmap protection. The special focussed on two main issues which was ignored by existing DCT based SE methods. They are rounding errors and recovery from non-selected DCT coefficients. They re-implemented previous work and presented the issue or rounding errors with a practical implementation. The rounding errors were due to truncation operations inside the DCT based SE. They cannot be ignored but multimedia contents can tolerate some level of noise introduced. They improved recovery methods that can recover visual elements of an image by guessing the DC coefficients from only a small set of known high frequency AC coefficients. It is shown that some published DCT based SE methods are not reliable for a high level of protection purpose. Gan Yu et,al (2014), presented a new image encryption algorithm is presented. In order to achieve security needs, an external secret key of 80-bit and two chaotic logistic maps are employed, and the initial conditions for the both logistic maps are derived by the external secret key. Firstly, the first logistic map is used to shuffle the position of plain-image pixels in the spatial-domain, so we can get shuffled image. Then the second logistic map is used to change grey value of shuffled image pixel and cipher-image appears. The relationship between the cipher-image and the plain-image is confused through the above two processes. The experimental results demonstrate that the proposed algorithm has large enough key space to resist all kinds of brute force attack and the distribution of grey value of the encrypted image. The proposed algorithm had three merits: (1) the algorithm has a large enough key space to resist all kinds of brute-force attacks; (2) the cipherimage has a good statistical property; (3) the encryption algorithm is very sensitive to the secret key.

Image protection with limited calculation resources environment

Han qiu et. al (2014), proposed an image protection with limited calculation resources environment with large amount images as input. Full traditional encryption of the data stream was not fast enough and takes too much CPU calculation resource in such an environment. They derived a new solution combined selective encryption with current GPGPU(General Purpose Graphic Process Unit) acceleration. After presenting related works, they introduce a new architecture and implementation of a selective encryption method by utilizing all calculation resources of a laptop including CPU and GPG. Yulen Sadourny et. al (2003), proposed selective encryption and impact of signalling information. Signalling is the key to interoperability in the JPEG-2000. Signaling of protection methods has been identified as keyto interoperability in JPSEC. When the signalling takes alsointo account the structure of the image codestream, it canprovide more information to transcoding applications, withlimited overhead. This has been demonstrated in this paper byapplying this principle to a selective encryption scheme. Thisproposal has been contributed to the JPSEC Ad hoc Group inApril 2003. At this stage, the signalling syntax and semantics was not yet finalized in the standard. Further cross-validations and experiments with other methods willsupport consensus building over the final syntax.

W. Puech et. al (2005), proposed a new scheme of partial or selective encryption for JPEG images based on AES cipher. It was based on encryption of some quantified DCT coefficients in low and high frequencies partial encryption is the approach to reduce computation resources for huge volume of multimedia data. They have combined encryption and compression and allow visualizationof the low-resolution compressed image. The experiments show that their method provides satisfactory PSNR, sufficient security and acceptable confidentiality results. Ayoub Massoudi et. al (2008), proposed selective encryption algorithm for JPEG2000 to reduce the amount of data to encrypt while achieving a sufficient and inexpensive security. This algorithm achieves the minimum encryption ratio required to achieve a target visual distortion while guaranteeing cryptographically secure selectively encrypted bitstream. This allows achieving important time saving. In future works, they will focus on compressing the metadata needed for decryption. They will also investigate the extensionof the proposed method to other compression standards such as H. 264 AVC/SVC.

FRWT domain based technique

Nidhi taneja et. al (2011), presented a FRWT domain based technique. Theyconsiders the inherent properties of image data and selectively encrypts only the significant part. To identify the significant data, relationship between NIE and perceptual information of a subband is derived. An increased effective key space is obtained by chaotic encryption of the selected subbands. This makes the fractional order, just a part of the key, but not

the most important key component. With the proposed technique, encryption of only 3. 125% of the entire image data leads to an acceptable perceptual security. The proposed technique provides high cryptographic security that is ascertained by considering the statistical and key-related attacks. Performance analysis in lossy and noisy communication channels demonstrate its robustness against eavesdropping and approximation attacks. Sattar B. Sadkhan et. al (2017), introduced the evaluation of RSA cryptosystem using Adaptive Neural Fuzzy Inference System. The ANFIS technique included hybrid between ANN and fuzzy logic techniques. This paper used 16 bytes plain text entered to RSA algorithm to get trained data which represented the values of used parameters such as key length, time complexity, key entropy, cipher text entropy. The code program of the algorithm was executed again on other 16 bytes plain text after simple change on the used key to get test matrix data. Then enter the data to ANFIS to train the data and get the security evaluation degree results, which represented the security level of RSA Algorithm. The ANFIS Evaluator provided a good security measure to some of the tested information security systems. The ANFIS Evaluator used 5 different parameters for each information security system as mentioned above. With those five parameters, the ANFIS evaluator could provide the exact evaluation for the tested RSA information security system. Purnima Gupta et. al (2018),proposed to analyze the existing data encryption schemes like RSA, AES KP-ABE, CP-ABE. The comparison among them were based on the computational cost and storage cost. They have also proposed to improve the scheme of improving the RSA encryption using multithreading concept on multi core CPU. The performance analysis helped the authors to know the difference between sequential and parallel RSA for encryption and decryption of files.

Study on keyword search-based and multi-keyword ranked search implementations

Harshitha. Y et. al (2017), provided a comparative study on keyword search-based and multi-keyword ranked search implementations with the intention of comparing them in terms of efficiency. The performance of these implementations were based on the speed of searches made over encrypted data with the same is extended in the view of decryption. They attempted to improve the search time efficiency of multi- keyword ranked search scheme over the RSA encryption and decryption analysis. By calculating all the graphs and statistical search efficiency tables . They could conclude that RSA Encrypted and Decrypted Scheme is more faster than Non Encrypted and Decrypted Scheme. The RSA Encrypted Scheme is gives better result than the existing and it is reducing the space complexity. Viney Pal Bansal et. al (2015), presented a hybrid Cryptosystem using RSA and Blowfish algorithm. This hybrid cryptosystem was considered for cloud computing where digital signature was must for user authentication. So, this technique provided features of both symmetric and asymmetric cryptography. So, the algorithm was secure and authentication enabled process which provided better security for cloud computing. Blowfish is unpatented so the cryptosystem is cost efficient. The hybrid RSA and blowfish encryption technique is implemented by VHDL. Shubhi Mittal et. al (2015),considered RSA algorithm for encryption and image steganography for data hiding using LSB technique. Implementing cryptography and steganography simultaneously strengthened the security manifolds by making it less vulnerable to malicious usage without compromising the statistical parameters like memory usage, time complexity and cost. Naga Hemanth et. al (2017), proposed RSA algorithm to provide security to the data we send and also securing the key that we encrypt the data. This paper consists of three stages, the first stage includes encryption of text using playfair cipher of 9x6 matrix. In the second stage, XOR operation is performed between the encrypted text and the key which it has been encrypted. In the final stage encryption of key is done using RSA algorithm and continued with a XOR operation between the encrypted text and the encrypted key. The final encrypted text and the new encrypted key is sent to the receiver to decrypt the original message. This proposed algorithm provides an extra layer of security to the existed algorithms.

Hybrid (RSA & AES) encryption algorithm

Vishwanath et. al (2017),presented Hybrid (RSA & AES) encryption algorithm to safeguard data security in Cloud. This paper mainly focuses on Secure Upload of data on cloud such that even the administrator is unaware of the contents, Secure Download of data in such a way that the integrity of data is maintained and Proper usage and sharing of the public, private and secret keys involved for encryption and decryption. It uses three different keys each for encryption as well as decryption. one is the public key, which is made available to all, the second one is the private key which lies only with the user. This has helped in avoiding any chances of repeated or redundant key. The main purpose behind using RSA and AES encryption algorithm is that it provides three keys i. e. public key for encryption, and private key and secret key for decryption. The biggest advantage it provides us is that the keys are generated on the basis of system

time and so no intruder can even guess them there by giving us increased security along with convenience and the data is very secure on cloud. Pachipala Yellamma et. al (2015), proposed a method for providing data storage and security in cloud using public key cryptosystem RSA. This paper focusing on issues relating to the cloud data storage methods and security in virtual environment. Data security is an important aspect of quality of service as a result, Security must be imposed on data by using encryption strategies to achieve secured data storage and accessBecause of opaqueness nature of cloud, it is still having security issues. The RSA provides the high security in high potential data encryption methodology.

Enhanced RSA algorithm

George Amalarethinam et. al (2017), proposed Enhanced RSA algorithm by dividing the file into several blocks. Encryption is done by using any one of the popular symmetric or asymmetric key algorithms such as AES, DES, RSA, Blowfish and Triple DES etc. , RSA algorithm which is a asymmetric key algorithm uses two different keys for encryption and decryption processes. The Key size can be varied to make the encryption process strong. Hence it is difficult for the attackers to intrude the data. The proposed algorithm reduces the time of encryption and decryption processes by dividing the file into blocks and enhances the strength of the algorithm by increasing the key size. This strength paves the way to store data in cloud by the users without any inconvenience. In future, the time spent for encryption and decryption can still be improved by using the concept of Addition chaining. Rohini et. al (2018),proposed hybrid RSA algorithmfor securing encryption of data over our cloud. . Here RSA is the asymmetric algorithm which makes use of 2 keys for encryption and decryption purpose. Security in cloud computing plays an important role. So in this paper they proposed a framework to alleviate security issues at the level authentication and storage level in cloud computing. Proposed system has better results than the existing system. In future they will further work on other security parameters.

Partially homomorphic cryptosystem

Peidong Sha et. al in (2016), proposed Partially homomorphic cryptosystem, based on the features of the RSA algorithm. Here RSA is the asymmetric algorithm which makes use of 2 keys for encryption and decryption purpose. Public key is used for encryption and private key is used for decyption. This encryption system first checks whether the values of the public key and private key generated during the encryption process contain prime number, then combines with the Pascal's triangle theorem and RSA algorithm model. The new cryptosystem satisfies fully homomorphic encryption in cloud computing. In this paper they designed the additional algorithm to obtain the characteristic of addition of the full homormorphic encryption.

REFERENCES

[1] A. Pommer and A. Uhl, "Selective encryption of wavelet-packet encoded image data: efficiency and security," *Multimedia Systems*,2003.

[2] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, and F. -O. Devaux, "Secure and low cost selective encryption for jpeg2000," in Multimedia, 2008.

[3] Dr. D. I. George Amalarethinam,H. Leena "Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud" in World Congress on Computing and Communication Technologies,2017.

[4] G. Yu, Y. Shen, G. Zhang, Y. Yang "A Chaos-based Color Image Encryption Algorithm", Sixth International Symposium on Computational Intelligence and Design,2013.

[5] H. Qiu,G. Memmi,X. Chen,andJ. Xiong,"DCcoefficientrecovery for JPEG images in ubiquitous communication systems," *Future Generation Computer Systems*,2019.

[6] H. Qiu and G. Memmi, "Fast selective encryption methods for bitmap images," International Journal of Multimedia Data Engineering and Management (IJMDEM), vol. 6, no. 3, pp. 51–69, 2015.

[7] H. Qiu, N. Enfrin, and G. Memmi, "A case study for practical is- sues of DCT based bitmap selective encryption methods," in *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*. IEEE, 2018.

[8] H. Qiu and G. Memmi, "Fast selective encryption method for bitmaps based on GPU acceleration," in Multimedia (ISM), 2014 IEEE International Symposium on. IEEE, 2014.

[9] Harshitha Y, Seema and Ms. Apoorva. k "Comparative Study on RSA Algorithm of Multikeyword Search Scheme over Encrypted Cloud Data ",in International Conference on Intelligent Computing and Control,2017.

[10] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "Big data analysis- based secure cluster management for optimized control plane in software-defined networks," *IEEE Transactions on Network and Service Management*, 2018.

[11] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu, "Spoofing-jamming attack strategy using optimal power distributions in wireless smartgrid networks", IEEETransactionsonSmartGrid,vol. 8,no. 5, pp. 2431–2439, 2017.

[12] L. Kuang, L. Yang, J. Feng, and M. Dong, "Secure tensor de- composition using fully homomorphic encryption scheme," *IEEE Transactions on Cloud Computing*,2015.

[13] L. Krikor, S. Baba, T. Arif, and Z. Shaaban, "Image encryption us- ing DCT and stream cipher," *European Journal of Scientific Research*, 2009.

[14] M. Abdmouleh,, A. Khalfallah and M. Bouhlel "A Novel Selective Encryption DWT-based Algorithm for Medical Images", 14th International Conference on Computer Graphics, Imaging and Visualization,2017.

[15] N. Taneja, B. Raman, and I. Gupta, "Selective image encryption in fractional wavelet domain," *AEU-International Journal of Electronics and Communications*,2011.

[16] Naga Hemanth P, Abhinay Raj N, Nishi Yadav "Secure Message Transfer using RSA algorithm and Improved Playfair cipher in Cloud Computing" in 2nd International Conference for Convergence in Technology,2017.

[17] Purnima Gupta,Deepak Kumar Verma and Aswani Kumar Singh "Improving RSA algorithm using multithreading model for outsourced data securityin cloud storage" in 8th International Conference on Cloud Computing, Data Science & Engineering,2018.

[18] Pachipala Yellamma, Challa Narasimham, Velagapudi sreenivas "Data Security in Cloud using RSA" 2013.

[19] Peidong Sha, Zhixiang Zhu "The Modification of RSA Algorithm to adapt Fully Homomorphic Encryption Algorithm in Cloud Computing" 2016.

[20] Rohini, Er Tejinder Sharma "Proposed hybrid RSA algorithm for cloud computing" inProceedings of the Second International Conference on Inventive Systems and Control, 2018.

[21] Shubhi Mittal, Shivika Arora and Rachna Jain "PData Security using RSA Encryption Combined with Image Steganography" 2016.

[22] Sattar B. Sadkhan, Farqad H. Abdulraheem "A Proposed ANFIS Evaluator for RSA Cryptosystem used in Cloud Networking" in International Conference on Current Research in Computer Science and Information Technology (ICCIT), Slemani – Iraq,2017.

[23] T. Xiang, C. Yu, and F. Chen, "Secure MQ coder: An efficient way to protect JPEG 2000 images in wireless multimedia sensor networks," Signal Processing: Image Communication, 2014.

[24] Viney Pal Bansal and Sandeep Singh "A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs", in Proceedings of 2015 RAECS UIET Panjab University Chandigarh ,2015.

[25] Vishwanath S Mahalle, Aniket K Shahade "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm" 2010.

[26] W. Puech and J. M. Rodrigues, "Crypto-compression of medical images by selective encryption of DCT," in *Signal Processing Con- ference, 2005 13th European*. IEEE, 2005.

[27] Y. Li, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data over-collection in smart city," IEEE Transactions on Computers, vol. 65, no. 5, pp. 1339–1350, 2016.

[28] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," Information Sciences, vol. 387, pp. 103–115, 2017.

[29] Y. Sadourny and V. Conan, "A proposal for supporting selective encryption in JPSEC," *IEEE Transactions on Consumer Electronics*,2003.

[30] Z. Shahid and W. Puech, "Visual protection of HEVC video by se- lective encryption of CABAC binstrings. " *IEEE Trans. Multimedia*,2014.

